Toward a Common Framework for Role-Based Access Control

Panel Chair:
David Ferraiolo, National Institute of Standards and Technology

Panelists:
1. Dr. Ravi Sandhu, George Mason University
2. Dr. Virgil Gligor, University of Maryland
3. Rick Kuhn, National Institute of Standards and Technology
4. Thomas Parenty, Sybase

Introduction

Role based access control has been used in computer systems for at least 20 years, but only within the past few years have rigorously defined general purpose Role-based Access Control (RBAC) models begun to appear. Lately, there has been great interest in RBAC. RBAC has captured the attention of major vendors and researchers. For instance RBAC properties are now being directly designed into database products and several articles from around the world immerged. To maintain this momentum and to allow RBAC to reach its full potential, we must approach RBAC from the perspective of enterprise computing in the commercial arena. In other words, how will RBAC help in providing cost-effective information technology solutions to carry out the business activities of enterprises? The recent flurry of activity in RBAC suggests that RBAC has the capability to serve security requirements that are not being met by currently available systems. The purpose of this panel is to discuss the current state of RBAC research and future directions in research and implementation of RBAC.

A role is chiefly a semantic construct forming the basis of access control policy. With RBAC, system administrators create roles according to the job functions performed in an enterprise, granting permission (access authorization) to those roles, then assigning users to the roles on the basis of their specific job responsibilities and qualifications. The benefits to an enterprise are ability to administratively specify and enforce enterprise specific security policies that can not be achieved using other methods of access control, and to dramatically streamline the typically burdensome process of authorization management.

Why are roles special?

The central notion of role-based access control is that users do not have discretionary access to enterprise objects, but instead access permissions are administratively associated with roles, and users are administratively made members of appropriate roles. It has been felt that this idea can greatly simplify management of authorization data while providing opportunity for great flexibility in specifying and enforcing enterprize specific protection policies. Roles can be created for various job positions in an organization. Users can be made members of roles as determined by their responsibilities and qualifications, and can be

easily reassigned from one role to another without modifying the underlying access control structures.

In some cases the potential benefits of RBAC have been accepted by both users and vendors, without a precise definition of what constitutes RBAC. In the past RBAC features have been implemented in enterprise applications, without a frame of reference as to its functional makeup, making RBAC an amorphous concept interpreted in different ways by users, researchers, and system developers.
There is a clear need to define and guide the evolution of a reference model for RBAC that is vendor neutral and mechanism independent and serve as a unifying force. From a commercial standpoint, we have to consider how RBAC fits into emerging models of computing, to include massive distribution such as internet, interoperable objects and software components, and workflow automation.

To promote the advancement and definition of RBAC the National Institute of Standards and Technology (NIST) is conducting and sponsoring research in the area of RBAC. To date three independently developed efforts on RBAC are underway at NIST: a Small Business Innovation Research (SBIR) program with Dr. Ravi Sandhu of George Mason University and Seta Corporation to help define RBAC and its feasibility, an effort with NSA's R23 Research and Engineering group and Dr. Virgil Gligor of the University of Maryland to create a formal model and implement RBAC on a policy-independent Mach microkernel-based operating system being developed by R23 called Synergy, and a Advanced Technology Program (ATP) effort being led by John Barkley of NIST to demonstrate how RBAC can be used for a health care system. As a result of these and other research efforts into RBAC, a number of well defined RBAC approaches and model have been created.

Common Model for RBAC

To date this RBAC research has yielded success in that advanced properties and models of RBAC are now widely available through numerous publications on the subject. In some cased viability of advanced RBAC features have been demonstrated through implementation and their application. There are even signs that some of the more advanced properties of RBAC are now being designed and implemented within significant and well established commercial products.

Although, the state of the technology has advance considerably over the past few years, there still does not exist a single or defacto standard for RBAC. Work is now being conducted to develop a consolidated model of RBAC that takes advantage of past and existing research. While there does exists a good amount of agreement as to what constitutes RBAC, many differences do exist.

An obvious question is whether there should be a common, widely accepted, model for RBAC, as there is for multi-level security. If

so, what model should be used? It is probably too early for a formal standard for RBAC, but we are likely to see a common model begin to emerge as industry implements role based systems. One RBAC specification that has already been implemented in commercial systems is included in the latest SQL3 database standard. But many applications have requirements that differ from database systems, so a general purpose model for RBAC may look different from that defined for SQL. For example, many applications may require dynamic separation of duty, which is not part of the SQL3 definition of RBAC. Other open consensus specifications with RBAC components include the Secure European System for Applications in a Multi-vendor Environment (SESAME), and the RBAC example included in the Object Management Group's Common Object Request Broker Architecture (CORBA).

The motivation for this panel is to publicly describe and compare some of the more prominent RBAC approaches that exist today.

It is expected that the panel members with their diverse backgrounds will bring both an industrial and academic perspectives to the discussion.